AU 99/1128
4

Patent Office
Canberra

I, LEANNE MYNOTT, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. PP 7764 for a patent by PORTUS PTY LTD filed on 17 December 1998.

WITNESS my hand this
Eighteenth day of February 2000

L. Mynott

LEANNE MYNOTT
TEAM LEADER EXAMINATION
SUPPORT AND SALES

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

AUSTRALIA

Patents Act 1990

PROVISIONAL SPECIFICATION

Applicant(s):

PORTUS PTY LTD

A.C.N. 084 990 090

Invention Title:

LOCAL AND REMOTE MONITORING USING A STANDARD WEB BROWSER

The invention is described in the following statement:

Local and Remote Monitoring Using a Standard Web Browser

Field of the Invention

The present invention relates to the area of local and remote monitoring and control, through use of a standard web browser and the Internet.

Background of the Invention

A communication node between data and a telecommunication networks is disclosed in PCT Patent Publication Number WO 94/24803 which describes a node that enables communication between users using different types of terminals, such as telephones and computers.

PCT Patent Publication Number WO 98/19445 describes a service node between Internet networks and a telecommunications network that is used to order telephony services by means of HTML pages from a computer with a WWW browser. It also describes a method of calling a subscriber, in which the call is ordered by computer but the connection is set up between the telephones of a first and second subscriber. The service node communicates with computers connected to computer networks using the HTTP protocol. The node stores data related to a subscriber; said data can be used when the user requests a telephony service.

A system for the control of devices within the home, using web browsers, is described in "Browser-style interfaces to a home automation network", IEEE Transactions on Consumer Electronics Volume 43 4, D. Corcoran, J. Desbonnet.

The automation and security systems that may be installed in a user's premises are becoming more and more advanced. Users often have a common need to control and monitor such systems both locally and remotely. Typically these systems provide an on-site control panel offering input facilities and visual status display facilities, but generally must resort to non-visual monitoring and control mechanisms for remote operation. Remote operation is usually achieved by telephone through codes entered via a

telephone handset. Some systems allow both local and remote operation using any combination of voice command input and voice feedback of status. Due to the complexity of the automation systems and the choices they afford users, such remote systems are cumbersome and limit the scope for interaction. In addition, the user must learn several alternate methods of control.

Another problem with current systems is the absence of a monitoring and control method that provides a geographically independent standard interface that is universally accessible and not platform or hardware dependant. Corcoran describes the use of a web browser and the WWW for a standard interface, both local and remote, in "Browser-style interfaces to a home automation network", IEEE Transactions on Consumer Electronics Volume 43 4,. However it is assumed in that paper that for remote monitoring and control, the site to be controlled is actively connected to the Internet at the time that remote operation is desired. In the case that the site is not actively connected to the Internet, a user may initiate a connection from their remote location to the desired site manually. However, this requires special knowledge and telecommunications access facilities on the part of the user and is not a suitable mechanism for those individuals who are not technically literate.

Another problem with current systems, and with the system described by Corcoran, is that if the user is geographically remote to the user premises, then initiating a direct connection through the public telecommunication network is expensive, requiring a long distance or international call.

Another problem with current systems relates to the handling of alarm and surveillance data. Current systems are based on CCTV and VCR technology. A problem associated with such systems is that surveillance data remains unprotected whilst retained at the site of an incursion.

Another problem with current systems relates to the cost associated with the surveillance system. System costs for video surveillance may be prohibitive, as they are based on CCTV and VCR technology. In addition, steps must be taken to ensure that surveillance data remains protected if it must be retained at the site of an incursion. Methods employed to make such systems tamper-proof add to the total system cost.

Another problem associated with current surveillance systems is that they may not differentiate alarm and non-alarm conditions, and continuously record activity. Such systems record in a loop fashion, eventually overwriting prerecorded material.

Another problem with current systems is that they do not allow, except in the case of expensive systems, a remote user, or remote authorized security personnel, to interrogate a surveillance or automation system during an alarm condition.

Another problem with existing systems is that they do not provide a facility for viewing surveillance material in relation to a user premises during non-alarm periods using standard platform independent and location independent mechanisms.

Summary of the Invention

In accordance with a first aspect of the present invention, there is provided an integrated system for monitoring and control, alarm detection and transmission, and alarm servicing, accessible both locally and remotely through a standard web browser interface via secure user-specific HTML pages comprising: an Internet access device for interconnecting with a provider network for remote operation; a provider network comprising: a TCP/IP network connected to the Internet with resources addressed by Universal Resource Locators (URLs); a user authentication system or database including user contact details; a user premises connection system or database; a user data storage system or database at least one service nodes at least one

communications servers at least one user private HTML pages interconnect with a user private storage area accessible through user private HTML pages and including user private premises connection method associated with user private HTML page; and a user premises network comprising at least: a gateway embodying a http server; one or more physical networks connected to the gateway; appliances connected to the physical network connected to the gateway where: secure access of a user private HTML page is intercepted by one of the service nodes which instructs one of the communications servers to establish a connection with the user premises gateway, the service node thereafter forwarding the intercepted URL request to the gateway, the gateway then executing the requested action by sending a monitoring or control command to the requested device on the user premises network, and thereafter relaying any requested information through HTML page back to user.

Alert conditions are preferably detected by appliances which can include user premises network sensors, or user premises network digital security camera, wherein alert condition are preferably transmitted to the gateway, wherein it can be optionally qualified with pre-programmed enable, and if result can be TRUE, an alarm event can be generated, whereupon the gateway establishes connection with the provider network, and surveillance data can be uploaded to provider network for secure storage accessible under the user's private storage area.

A service node can ideally be located within the local telephone call radius of the user premises, thus providing lowest cost PSTN access from or to user premises. When a non-local service node is used, particularly a centralised service node, a low cost access can be provided through special carrier arrangements.

The resulting integrated and distributed surveillance monitoring network, allows for centralised remote monitoring by authorised monitoring personnel through a web browser interface to secure provider

extranet.

A system can provide for photos of user premises are preferably accessible from a database and that may be retrieved upon alarm event and cross referenced with surveillance data to ascertain whether a true alarm has been raised.

Ideally. authentication is required only once, and thereafter when accessing the same address on the provider network from the same internet access device, authentication information stored within the Internet access device can be automatically rechecked and need not be re-entered. The authentication can be handled by a CGI.

Publicly accessible HTML pages are preferably additionally provided for each user and the provider network can provide a user premises email facility, and automatically raises connection in a pre-programmed fashion to premises and transfers user email to the gateway.

The internet access device preferably can include a smart card reader, and where smart card provides authentication details and URL corresponding to user premises through the provider network. The smart card also facilitates global access to Internet for access of provider network, and optionally additionally tracks connections for expensing.

The Internet access device can be a computer, WebPhone, Portable digital assistant, or mobile phone with web browsing capability.

The gateway can incorporate a user programmed answer strategy, including delayed answer, and optionally detects a voice connection and record compressed version, thus operating in answering machine mode such that upon answering the incoming call, the gateway raise a connection to the provider network, and send an indication to the user of the recorded message, and that sends recorded compressed voice messages to remote user upon request. The gateway can provide indication of messages received on HTML page, so that user can be notified via the premises control

terminal. Further, the gateway can detect a fax and stores the fax.

The gateway can be in a tamperproof enclosure, and operates without mains power and can trigger an alarm and relay alarm to the provider network in case of attempted tampering.

The gateway normally acts as a hub and internet connection mechanism for connected devices on user premises network.

A control terminal can be provided comprising a wall mounted flat panel display incorporating a touch screen and a user premises physical network connection, and running web browser. The control terminal can be equipped with biosensor, preferably in form of fingerprint sensor, for access authentication of local user. The control terminal can be preferably connected to a wireless user premises network and can be powered by rechargeable batteries, allowing the control terminal mobility within the range of wireless transmitters attached to the user premises network. The control terminal can be of reduced handheld size, so that it can operate as universal premises remote control. Further, the terminal can integrate a digital camera, microphone and speaker, and H.324 protocol software, thus allowing the control terminal to be used as a videophone, through standard browser interface. Alternatively, the control terminal can be provided by a standard PC equipped with user premises network connection via an installed adaptor, wherein the PC can be running a browser accessing URL corresponding to the gateway. Alternatively, the control terminal can be provided by set top box connected to TV and running web browser, with connection to the user premises network. Further, the control terminal it can be equipped with smartcard reader, thus enabling ecommerce transactions.

The gateway can be programmable to allow different response mechanisms to differing classes of alert event. A database in the gateway can contain connection

details for preferred and secondary communication servers on the provider network, so that if primary communication does not respond, secondary servers may be contacted until successful connection can be achieved.

The user data storage system can be centralised or distributed, with storage made on fixed basis per user or allocated virtually and redundantly.

The user contact database preferably can include preferred contact methods, allowing automatic contact mechanisms to be associated with alarm condition, including use of email, pager, computer generated voice message through telephone, requesting response or if timeout, security action.

At least one of the appliances can comprise a digital security camera embodying image capture and compression method and user premises network interface.

The camera can include motion detection and image significance algorithms which run in the camera, and filter input so that only relevant input can be compressed and sent through gateway to provider network.

A least one of the appliances can be an external access mechanism to the user premises equipped with a reader for a RF tag that can be used for user authentication or equipped with a smartcard reader that can be used for user authentication. Alternatively, the external access mechanism can include a biosensor, preferably a fingerprint sensor, attached to the substrate of the smart card, and circuit embedded in smartcard to authenticate user before the smartcard will operate.

The gateway service module can provide support for the HomePnP standard for CEBus networks, and support for the HAVi standard for consumer appliance control.

The present invention attempts to simplify the use, for a user, of automation and security services in relation to their premises. It achieves this simplification of use by providing an integrated facility for monitoring and control, alarm detection and

transmission, and alarm servicing, that is accessible both locally and remotely through a standard web browser via secure user-specific HTML pages. The present invention is equally applicable to a range of premises types, including, but not limited to the home, business premises, rural, industrial and government facilities. In the descriptions that follow, the terms user's premises or user premises indicate a premises that the user wishes to monitor or control.

The present invention provides a uniform method of monitoring and control using a web browser interface making the remote connection procedure transparent to the user requiring no training beyond that required to use a web browser. This facility is achieved by providing an Internet-connected service node, which initiates a telecommunications connection, via either a public telecommunications network or a private network, to the user premises gateway upon access of a specific user private HTML page dedicated to this purpose.

The present invention attempts to simplify the use, for a user, of automation and security services in relation to their premises. It also simplifies monitoring of the user premises by an authorised security service. It achieves this simplification of use by providing an integrated facility for monitoring and control, alarm detection and transmission, and alarm servicing, that is accessible both locally and remotely through a standard web browser via secure user-specific HTML pages.

The present invention provides inexpensive remote connection, by utilizing an Internet connection that is local to the user and consequently accessed at a lower cost. The present invention circumvents the surveillance data protection problem by storing data through the Internet in a secure repository offsite from the user premises being monitored. The present invention allows for a reduction in cost by separating the surveillance requirement into imaging, compression and storage elements,

with only the imaging and compression mechanisms located at the user premises, and by locating the expensive data storage element at a remote centralised location. The integrity of surveillance stored in such a manner may be enhanced using storage redundancy mechanisms, thus conveying a further advantage over existing systems. By employing digital image capture and compression technology, storage costs are further reduced, especially in relation to the total storage capacity consumed by a surveillance event. The present invention reduces storage requirements by providing a central repository that provides storage of surveillance data for multiple users, so that total storage is shared amongst users, and rather than providing a fixed pre-determined storage capacity for each user, virtual storage allocation is possible. Further, present invention can be adapted to record only when triggered, or as otherwise programmed to do so, so that the period of surveillance that may be retained is increased.

The present invention can include an Internet based automation and surveillance system includes a provider network accessible through the Internet. An authorised user accesses the provider network, through its associated URL, using an Internet access device connected to the Internet. (user must login) The provider network (* extranet or private network) includes a number of resources distributed among the nodes that form the network. The resources include user private storage repositories, user private HTML pages, service nodes and communications servers. Each premises serviced by the provider network is associated with a primary (and secondary) service node located within the provider network. A unique URL corresponds to the address of a gateway at the user premises, and falls under the address hierarchy of a service node. A request to access the URL corresponding with the gateway at the user premises is detected by the service node, which instructs a communications server to establish a connection with the user premises gateway. Once a connection is established

between the user premises and the provider network, the previously requested URL is relayed to the gateway, wherein it is serviced by a web server running on the gateway. A service module running on the gateway interprets requests for monitoring and control and directs these requests to the device selected within the user premises network, and formats status data for delivery back through HTML pages to user.

An alert condition may be detected by appliances on the user premises network, in form of sensors, or digital compressed security camera, and alert condition transmitted to the gateway, wherein it is optionally qualified with pre-programmed enables, and if result is TRUE, an alarm event is generated, the gateway establishes connection with provider network, a monitoring station is automatically informed, and surveillance data is uploaded to the provider network for secure storage accessible under user's private storage area.

The present invention makes it possible to economically view surveillance data at the time of the event, whether such data consists of images or video, remotely for appraisal of the severity of the alarm condition.

Brief Description of the Drawings

Preferred embodiments of the present invention will now be described with reference to the accompanying drawings in which:

Fig. 1 illustrates a TCP/IP protocol stack;

Fig. 2 illustrates an internet HTTP query and answer;

Fig. 3 illustrates the arrangement of the preferred embodiment;

Fig. 4 illustrates the software modules of a gateway;

Fig. 5 illustrates a gateway attached to a series of appliance via different networks;

Fig. 6 illustrates a gateway attached to a series of appliances;

Fig. 7 illustrates schematically the structure of a first camera system;

Fig. 8 illustrates schematically the structure of a second camera system;

Description of Preferred and Other Embodiments

The preferred embodiments provide a method of remote control that provides the user visual monitoring and control information. The preferred embodiment also provides a visual interface for both remote and local monitoring and control. The preferred embodiment simplifies the use, for a user, of automation and security services in relation to their designated premises. It also simplifies monitoring of the user premises by an authorised security service. It achieves this simplification of use by providing an integrated facility for monitoring and control, alarm detection and transmission, and alarm servicing, that is accessible both locally and remotely through a standard web browser via secure user-specific HTML pages.

In order to more clearly describe the preferred embodiment the following terms are defined:

TCP/IP: (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in the private networks called intranets and in extranets. This protocol suite is commonly held to be composed of different layers to enable an open systems interconnection architecture. There is no agreement on exactly how many layers are used to describe the suite though most references use from three (3) to five (5) functional levels within the suite. The four (4) level model as shown in Fig. 1. is based on three (3) layers (Application, Host-to-Host, and Network Access) with the inclusion of a separate Internet Layer. As with the International Standards Organisation (ISO) Open Systems Interconnect (OSI) model the data is passed down the layers (protocol stack) from the Application Layer to the underlying physical network. Each layer provides additional

control information to ensure proper delivery of the information to the interconnected system. Each layer treats information from the layer above as data and places its own header in front of the data. When the information is received at the interconnected system the data passes up through the layers and at each level the information received is treated as both header and data, with the header removed and the data passed to the next layer up.

Internet: The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer. It was conceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first known as the ARPANet. The original aim was to create a network that would allow users of a research computer at one university to be able to "talk to" research computers at other universities. A side benefit of ARPANet's design was that, because messages could be routed or rerouted in more than one direction, the network could continue to function even if parts of it were destroyed in the event of a military attack or other disaster. Today, the Internet is a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people worldwide. Physically, the Internet uses a portion of the total resources of the currently existing public telecommunication networks. Technically, what distinguishes the Internet is its use of a set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol). Two recent adaptations of Internet technology, the intranet and the extranet, also make use of the TCP/IP protocol. The most widely used part of the Internet is the World Wide Web (often abbreviated "WWW" or called "the Web"). Its outstanding feature is hypertext, a method of instant cross-referencing. Using the Web, you have access to millions of pages of information. Web "surfing" is done with a Web browser, the most popular of which are Netscape

Navigator and Microsoft Internet Explorer.

Intranet: An intranet is a network of networks that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in a wide area network. Typically, an intranet includes connections through one or more gateway computers to the outside Internet. The main purpose of an intranet is to share company information and computing resources among employees. An intranet uses TCP/IP, HTTP, and other Internet protocols and in general looks like a private version of the Internet. With tunneling, companies can send private messages through the public network, using the public network with special encryption/decryption and other security safeguards to connect one part of their intranet to another.

Extranet : An extranet is a private network that uses the Internet protocols and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company. It has also been described as a "state of mind" in which the Internet is perceived as a way to do business with other companies as well as to sell products to customers. An extranet requires security and privacy. These require firewall server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages, and the use of virtual private networks (VPNs) that tunnel through the public network.

VPN: A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The idea of the VPN is to give the company the same capabilities at

much lower cost by sharing the public infrastructure. Phone companies have provided secure shared resources for voice messages. A virtual private network makes it possible to have the same secure sharing of public resources for data. Companies today are looking at using a private virtual network for both extranets and wide-area internets. Using a virtual private network involves encrypting data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses.

HTTP: The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol. Fig. 2 illustrates a standard internet transaction with a client 10 sending a query to a server 11 which in turn sends a html script back to the client 10. The query and replied utlize the TCP/IP protocols 13 to perform the transaction.

Web Server: A HTTP Server.
Web Browser: A HTTP Client.

URL: A URL (Uniform Resource Locator) is the address of a file (resource) accessible on the Internet. The type of resource depends on the Internet application protocol. Using the World Wide Web's protocol, the Hypertext Transfer Protocol (HTTP) , the resource can be an HTML page, an image file, a program such as a CGI application or Java applet, or any other file supported by HTTP. The URL contains the name of the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

HTML: (Hypertext Markup Language) is the set of

"markup" symbols or codes inserted in a file intended for display on a World Wide Web browser. The markup tells the Web browser how to display a Web page's words and images for the user. HTML is defined officially for the industry by the World Wide Web Consortium (W3C).

WWW: A technical definition of the World Wide Web is: all the resources and users on the Internet that are using the Hypertext Transport Protocol (HTTP).

Turning now to Fig. 3, there is illustrated the arrangement of the preferred embodiment which includes the following components;

An Internet access device 15, which may include, but is not limited to, a computer, a mobile phone with display, a Web Phone, or a Personal Digital Assistant, capable of connection to the World Wide Web (WWW) through a client web browser supporting the HyperText Transfer Protocol (HTTP).

A web browser interface which runs on the Internet access device and that allows the user to access, through queries over the WWW, HTML pages from HTTP servers corresponding to associated URLs.

An active Internet connection that connects the Internet access device 15 to the Internet 16.

A virtual private network (VPN) 17, termed here the provider network, which is connected to the Internet and which embodies a collection of Internet-accessible resources that implement part of the integrated monitoring and control, alarm transmission and servicing functions of the invention. This network 17, whilst accessible from the Internet, forms an Extranet.

The resources associated with the provider network (Fig. 3) including:

An authentication system or database 18 containing access information in relation to authorized users.

A user connection system or database containing connection parameters in relation to the user premises.

A login facility 19 to initiate a secure connection for authorized users.

User specific HTML pages which are linked to private areas, and possibly public areas.

A service node 20 which uses the user connection parameters to direct a communications server 21 to establish a connection through either a private or public telecommunications network to a gateway 22 at the user premises.

A communications server 21.

A telecommunications network 24.

A user premises gateway 22.

A web server running on the user premises gateway 22.

A home network 26 attached to the gateway, which may include sub nets of differing physical implementation. Appliances 27 attached to the home network which may be monitored and controlled.

Specific intrusion detection devices which may instigate alarms.

A surveillance device 28 in the form of a digital security camera.

A control terminal 29.

The following situations for operation of the preferred embodiment are identified:

1. The user is in a remote location with respect to their premises and wishes to monitor and control, or retrieve recorded data associated with, their premises;

2. The user is local to their premises and wishes to monitor and control their premises;

3. An alarm condition is reported to the monitoring network, and surveillance data recorded.

1. REMOTE OPERATION

The user premises network 26 is normally in an unconnected state in relation to the provider network 17. Specific actions on the part of the remote user, or their authorized agents, connect the user premises network to the

provider network, thus allowing monitoring and control operations to proceed.

Each user registered with the provider network has login data and premises connection data stored respectively in user login and user connection systems or databases 18 located within the provider network. In addition, private HTML pages 19 are provided for each user, allowing access to URLs dedicated to either of two resource classes. One resource class is dedicated to stored surveillance data, whilst the other resource class is dedicated to active connection to the user premises for monitoring and control.

A remote user, who desires to monitor or control their premises, uses a web browser on an Internet access device 15 to view the private HTML pages that are dedicated to monitoring and control of the user premises by entering a URL associated with the HTML page they wish to access.

Before the remote user may view the particular HTML pages that are associated with the monitoring and control of the user premises, they must first identify themselves to the provider network via a login procedure associated with the HTML pages in question. Once the user's identification details, constituting a user name and password are authenticated, the user is permitted access to the HTML page requested.

Once the user authentication process is complete, the records associated with the user, detailing connection parameters for the user premises, are retrieved from a database 18 in the provider network. The process of accessing the URL dedicated to the monitoring and control of the user premises initiates a sequence of events that culminate in connection of the user premises network 26 to the provider network 17. A service node 20 within the provider network intercepts the access to the URL dedicated to the monitoring and control of the user premises, and uses the premises connection data associated with the user to instruct a communications server 21 to initiate a

connection to the gateway 22 at the user premises

The communications server 21 at the service node interprets the user connection parameters and initiates a connection phase across the telecommunications facility to connect with the gateway 22 at the customer premises. The telecommunications facility 24 includes any system that allows end to end communication, including but not limited to the PSTN, PLMN, ISDN and RF communication.

Preferably, a gateway 22 at the user premises has a dedicated port to the telecommunications network. However, it is possible for the gateway to share the port to the telecommunications network, in which case the user may conure the gateway using a number of different response mechanisms, including a delayed answer mechanism.

The gateway answers the incoming call and completes the connection. The gateway and the connection server negotiate connection parameters and establish a network connection between the user premises network and the provider network. A web server on the gateway then accepts HTTP protocol through the connection. The service node 20 forwards the URL that was previously intercepted and that corresponds to a resource contained within the customer premises network to the gateway.

Turning now to Fig. 4 there is illustrated the components running on the gateway computer 22 in more detail. The computer includes a HTTP server 30 which runs as an application. The gateway web server 30 then serves information in relation to user premises appliances through HTML pages to the user. The gateway web server communicates with a Services Module 31, which allows the control and monitoring actions to be performed, and issues requests to the Services Module 31 to fulfil the user requests. The requests are relayed through the protocol stack 34 attached to the operating system resident in the gateway to the target appliances attached to the network. Data is sent or received from the device is response to the requests. In the case of control actions, the device performs the

action, whilst in the case of monitoring actions, the device returns the requested data.

As illustrated in Fig. 5, the gateway can be interconnected to a series of appliances 40 over a number of different networks 41, 42, 43. Fig. 7 illustrates one form of hardwired interconnection with a series of appliances 27.

2. LOCAL OPERATION

A local user can monitor and control devices and appliance in the user premises through a control terminal incorporating a display and an input mechanism. The control terminal can be implemented as a wall mounted display unit 45, a set top box and TV 46, or a PC 45, which runs a web browser. The user accesses HTML pages on the gateway 22 which provide monitoring and control services for devices located within the user premises that are attached to the premises network.

The gateway web server serves information through HTML pages to the user. The gateway web server communicates with a Services Module, which allows the control and monitoring actions to be performed, and issues requests to the Services Module to fulfil the user requests. The requests are relayed through the protocol stack attached to the operating system resident in the gateway to the target appliances attached to the network. Data is sent or received from the device is response to the requests. In the case of control actions, the device performs the action, whilst in the case of monitoring actions, the device returns the requested data.

3. ALARM OPERATION

Devices, such as sensors 49, attached to the user premises network may generate alert conditions, in response to a condition detected by a device sensor or to a particular device state. A special case identified is an alert condition generated by an intrusion detection or surveillance device.

A digital security camera 28 is provided and, as

shown in more detail in Fig. 7, incorporates an imaging device 50 for capturing an image, preprocessing unit 51, memory store 52, compression unit 53, network interface 54 and CPU 55. The digital security camera is connected to the user premises network gateway through a physical network. The gateway 22 and the camera system 28 communicate through a common protocol. The imaging device 51 within the digital security camera continuously records image data, which is then read from the imaging device, through the pre-processing circuit 51, and written to memory store 52. A compressor 53 reads image data from memory and produces a compressed version of the image data. The CPU 55 may optionally analyse the raw image using motion detection and image significance algorithms programmed into the CPU. If the security system is armed, and a significant event is detected, an alert condition is generated and compressed images and other information are transmitted through the network interface 54, across the user premises network, to the gateway 22.

In another embodiment of the security camera, as shown in Fig. 8, the functionality of the gateway is incorporated directly into the camera and a telecommunications interface 57 is provided for direct connection with the communications server.

Returning to Fig. 3, generally, once an alert condition is detected by a sensor or other device attached to the user premises network, information regarding the alert condition is transmitted via the user premises network 26 to the gateway 22. Software on the gateway interprets the information in relation to the alert condition, and may qualify the alert condition with user pre-programmed qualifiers stored in a database on the gateway 22. An alarm condition is generated if the logical AND of the alert condition and corresponding qualifier is TRUE. In response to an alarm condition, the gateway 22 uses pre-programmed connection parameters to initiate a connection through the telecommunications network 24 to a

preferred communications server 21 on the provider network 17. The communications server answers the call and completes the connection. If there is a fault and a successful connection to the communications server can not be raised, the gateway may retrieve from a local database further connection details for alternative communication servers on the provider network. Once a successful connection exists between the gateway and a communication server on the provider network, the gateway and the communication server negotiate connection parameters and establish a connection between the user premises network 26 and the provider network. This process identifies the user premises network, and hence the associated user, to the provider network 17. Information in relation to the alarm condition is transmitted from the user premises network 26 to the provider network 17. Software running on the provider network processes the alarm condition, and transmits an alarm state to a monitoring console. In addition, pre-programmed alarm actions in relation to the user are retrieved from a user database 18 on the provider network, and all actions identified are automatically performed. These may include automatic notification of the alarm condition to the user through mechanisms such as, but not limited to: email, pager, and telephone. In addition, all data associated with the alarm condition transmitted from the user premises network to the provider network is stored in a secure repository within the provider network. User pre-programmed qualifiers may gate access to this recorded surveillance data by authorized monitoring personnel. The data is accessible to the user in their private storage area, and may be viewed from their web browser.

It would be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the preferred embodiment without departing from the spirit or scope of the invention as broadly described. The preferred embodiment is,

therefore, to be considered in all respects to be illustrative and not restrictive.

We Claim

An integrated system for monitoring and control, alarm detection and transmission, and alarm servicing, accessible both locally and remotely through a standard web browser interface via secure user-specific HTML pages comprising:

an Internet access device for interconnecting with a provider network for remote operation;

a provider network comprising:

a TCP/IP network connected to the Internet with resources addressed by Universal Resource Locators (URLs);

a user authentication system or database including user contact details;

a user premises connection system or database;

a user data storage system or database

at least one service nodes

at least one communications servers

at least one user private HTML pages interconnect with a user private storage area accessible through user private HTML pages and including user private premises connection method associated with user private HTML page; and

a user premises network comprising at least:

a gateway embodying a http server;

one or more physical networks connected to the gateway;

appliances connected to said physical network connected to the gateway where: secure access of a user private HTML page is intercepted by one of said service nodes which instructs one of said communications servers to establish a connection with the user premises gateway, the service node thereafter forwarding the intercepted URL request to the gateway, the gateway then executing the requested action by sending a monitoring or

control command to the requested device on the user premises network, and thereafter relaying any requested information through HTML page back to user.

2. A system as claimed in claim 1 wherein alert conditions are detected by appliances which include user premises network sensors, or user premises network digital security camera, wherein alert condition are transmitted to said gateway, wherein it is optionally qualified with pre-programmed enable, and if result is TRUE, an alarm event is generated, whereupon said gateway establishes connection with the provider network, and surveillance data is uploaded to provider network for secure storage accessible under said user's private storage area

3. A system as claimed in claim 1, wherein a service node is located within the local telephone call radius of the user premises, thus providing lowest cost PSTN access from or to user premises

4. A system as claimed in claim 1, wherein when a non-local service node is used, particularly a centralised service node, and low cost access is provided through special carrier arrangements

5. A system as claimed in claim 1, providing an integrated and distributed surveillance monitoring network, allowing centralised remote monitoring by authorised monitoring personnel through web browser interface to secure provider extranet

6. A system as claimed in any previous claim, wherein photos of user premises persons are accessible from a database and that may be retrieved upon alarm event and cross referenced with surveillance data to ascertain whether a true alarm has been raised

7. A system as claimed in claim 1, wherein authentication is required only once, and thereafter when accessing the same address on the provider network from the same internet access device, authentication information stored within the Internet access device is automatically rechecked and need not be re-entered.

8. A system as claimed in any previous claim, wherein authentication is handled by a CGI

9. A system as claimed in any previous claim, wherein publicly accessible HTML pages are additionally provided for each user.

10. A system as claimed in any previous claim wherein provider network provides a user premises email facility, and automatically raises connection in a pre-programmed fashion to premises and transfers user email to said gateway

11. A system as claimed in any previous claim wherein the internet access device includes a smart card reader, and where smart card provides authentication details and URL corresponding to user premises through provider network.

12. A system as claimed in claim 11, wherein said smart card also facilitates global access to Internet for access of provider network, and optionally additionally tracks connections for expensing.

13. A system as claimed in any previous claim, wherein the Internet access device is a computer, WebPhone, Portable digital assistant, or mobile phone with web browsing capability.

14. A system as claimed in any previous claim wherein the gateway incorporates a user programmed answer strategy, including delayed answer, and optionally detects a voice connection and record compressed version, thus operating in answering machine mode.

15. A system as claimed in claim 14, wherein upon answering the incoming call, the gateway raise a connection to the provider network, and send an indication to the user of the recorded message, and that sends recorded compressed voice messages to remote user upon request.

16. A system as claimed in claim 14, wherein the gateway provides indication of messages received on HTML page, so that user is notified via the premises control

terminal.

17. A system as claimed in any previous claim, wherein the gateway detects a fax and stores the fax.

18. A system as claimed in any previous claim, wherein the gateway is in a tamperproof enclosure, and operates without mains power.

19. A system as claimed in any previous claim , wherein the gateway is tamperproof, and triggers an alarm and relay alarm to the provider network in case of attempted tampering.

20. A system as claimed in any previous claim, wherein the gateway acts as a hub and internet connection mechanism for connected devices on user premises network.

21. A system as claimed in any previous claim further comprising a control terminal comprising a wall mounted flat panel display incorporating a touch screen and a user premises physical network connection, and running web browser.

22. A system as claimed in any previous claim wherein the control terminal is equipped with biosensor, preferably in form of fingerprint sensor, for access authentication of local user.

23. A system as claimed in any previous claim, wherein the control terminal is preferably connected to a wireless user premises network.

24. A system as claimed in any previous claim, wherein the control terminal is powered by rechargeable batteries, allowing the control terminal mobility within the range of wireless transmitters attached to the user premises network.

25. A system as claimed in any previous claim, wherein control terminal is of reduced handheld size, so that can operate as universal premises remote control.

26. A system as claimed in any previous claim, wherein the terminal integrates a digital camera, microphone and speaker, and H.324 protocol software, thus allowing the control terminal to be used as a videophone,

through standard browser interface.

27. A system as claimed in any previous claim, wherein a control terminal is provided by standard PC equipped with user premises network connection via an installed adapter, wherein PC is running browser accesses URL corresponding to gateway.

28. A system as claimed in any previous claim, wherein a control terminal is provided by set top box connected to TV and running web browser, with connection to user premises network

29. A system as claimed in any previous claim, wherein the control terminal it is equipped with smartcard reader, thus enabling ecommerce transactions.

30. A system as claimed in any previous claim wherein at least one of said appliances comprises a digital security camera embodying image capture and compression method and user premises network interface.

31. A system as claimed in any previous claim wherein at least one of said appliances comprises a digital security camera embodying image capture and compression methods and an internet connection.

32. A system as claimed in any previous claim 30 or 31 wherein said camera incluldes motion detection and image significance algorithms which run in said camera, and filter input so that only relevant input is compressed and sent through gateway to provider network.

33. A system as claimed in any previous claim wherein said gateway is programmable to allow different response mechanisms to differing classes of alert event.

34. A system as claimed in any previous claim wherein a database in said gateway contains connection details for preferred and secondary communication servers on said provider network, so that if primary communication does not respond, secondary servers may be contacted until successful connection is achieved.

35. A system as claimed in any previous claim wherein said user data storage system is centralised or

distributed.

36. A system as claimed in any previous claim wherein said user data storage is made on fixed basis per user.

37. A system as claimed in any previous claim wherein said user data storage is allocated virtually.

38. A system as claimed in any previous claim wherein said user data storage is allocated reduntantly, ensuring integrity of stored surveillance data.

39. A system as claimed in any previous claim wherein the user contact database includes preferred contact methods, allowing automatic contact mechanisms to be associated with alarm condition, including use of email, pager, computer generated voice message through telephone, requesting response or if timeout, security action.

40. A system as claimed in any previous claim, wherein at least one of said appliances is an external access mechanism to said user premises.

41. A system as claimed in any previous claim, wherein at least one of said appliances is equipped with reader for RF tag that is used for user authentication.

42. A system as claimed in any previous claim, wherein at least one of said appliances is equipped with a smartcard reader that is used for user authentication.

43. A system as claimed in any previous claim, wherein said gateway service module provides support for the HomePnP standard for CEBus networks, and support for the HAVi standard for consumer appliance control.

44. A system as claimed in claim 42, wherein the smartcard includes a biosensor, preferably a fingerprint sensor, attached to the substrate of the smart card, and circuit embedded in smartcard to authenticate user before the smartcard will operate.

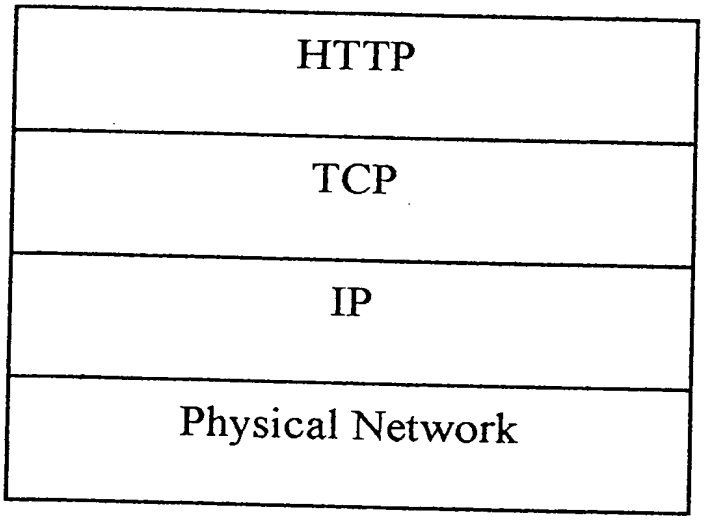

FIG. 1

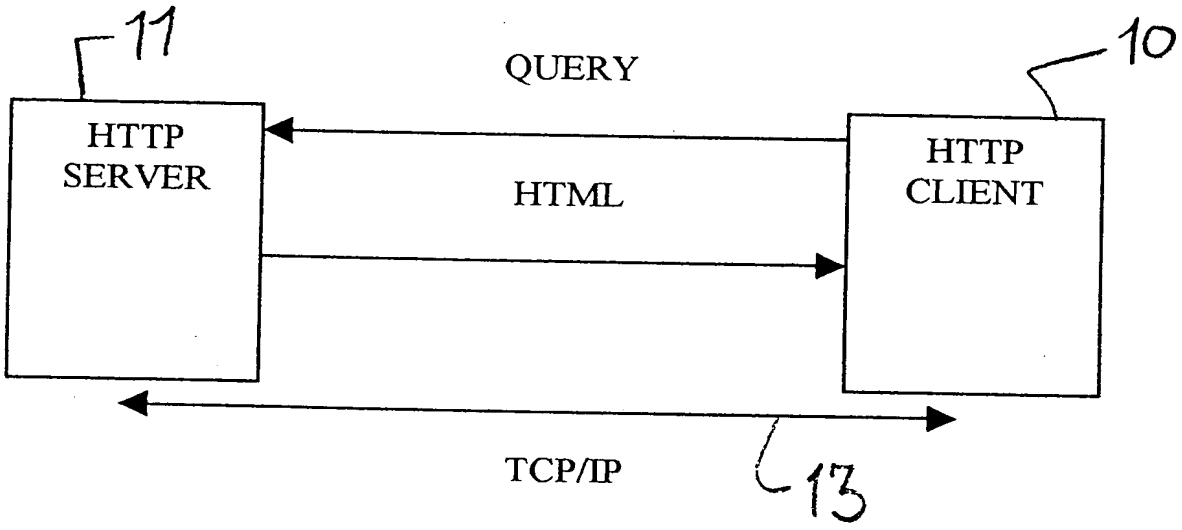

FIG. 2

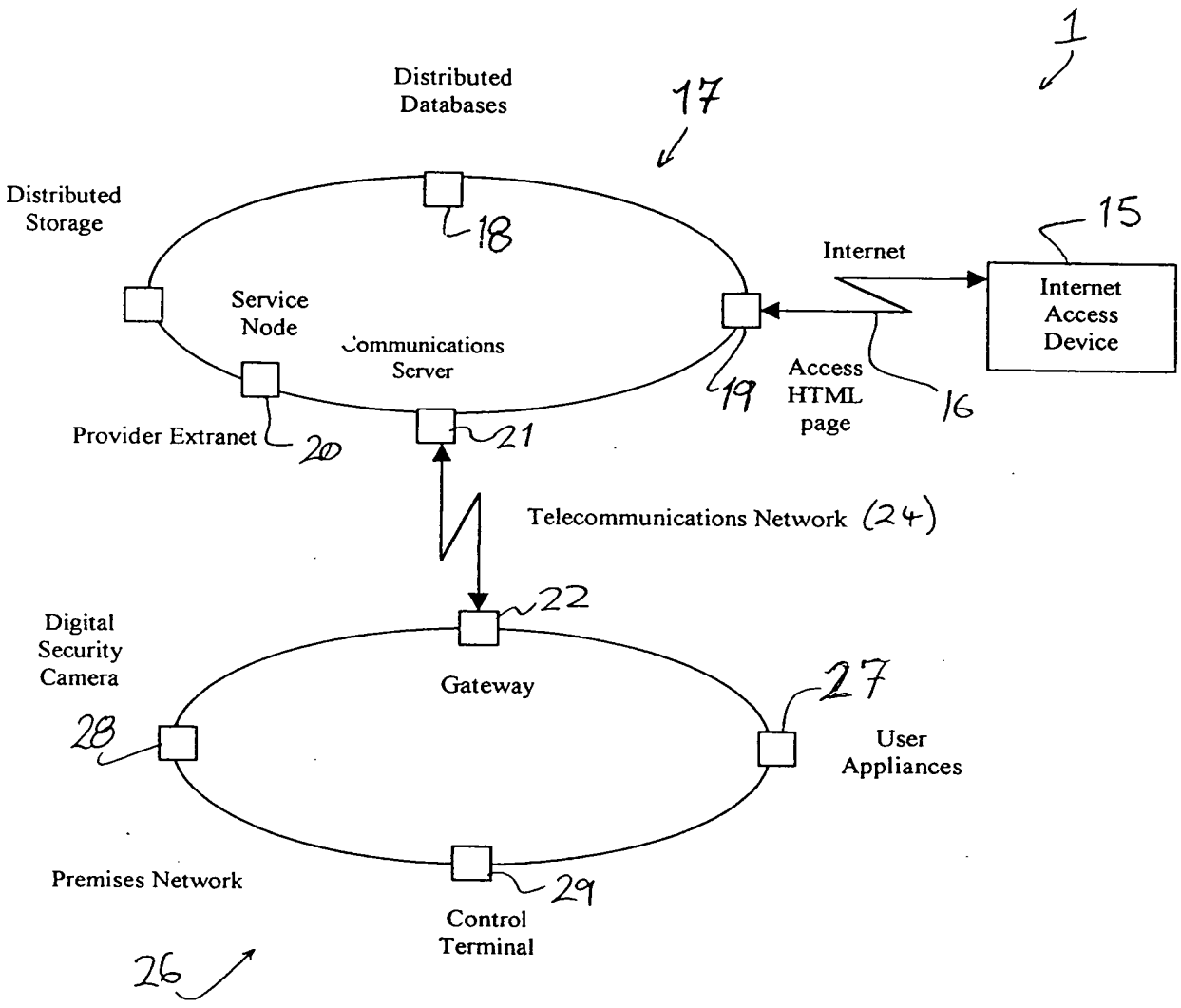
1
Distributed Databases
17
Distributed Storage
18
Service Node
Communications Server
19
Internet
15
Internet Access Device
Access HTML page
16
Provider Extranet
20
21
Telecommunications Network (24)
22
Digital Security Camera
28
Gateway
27
User Appliances
Premises Network
29
Control Terminal
26

FIG. 3

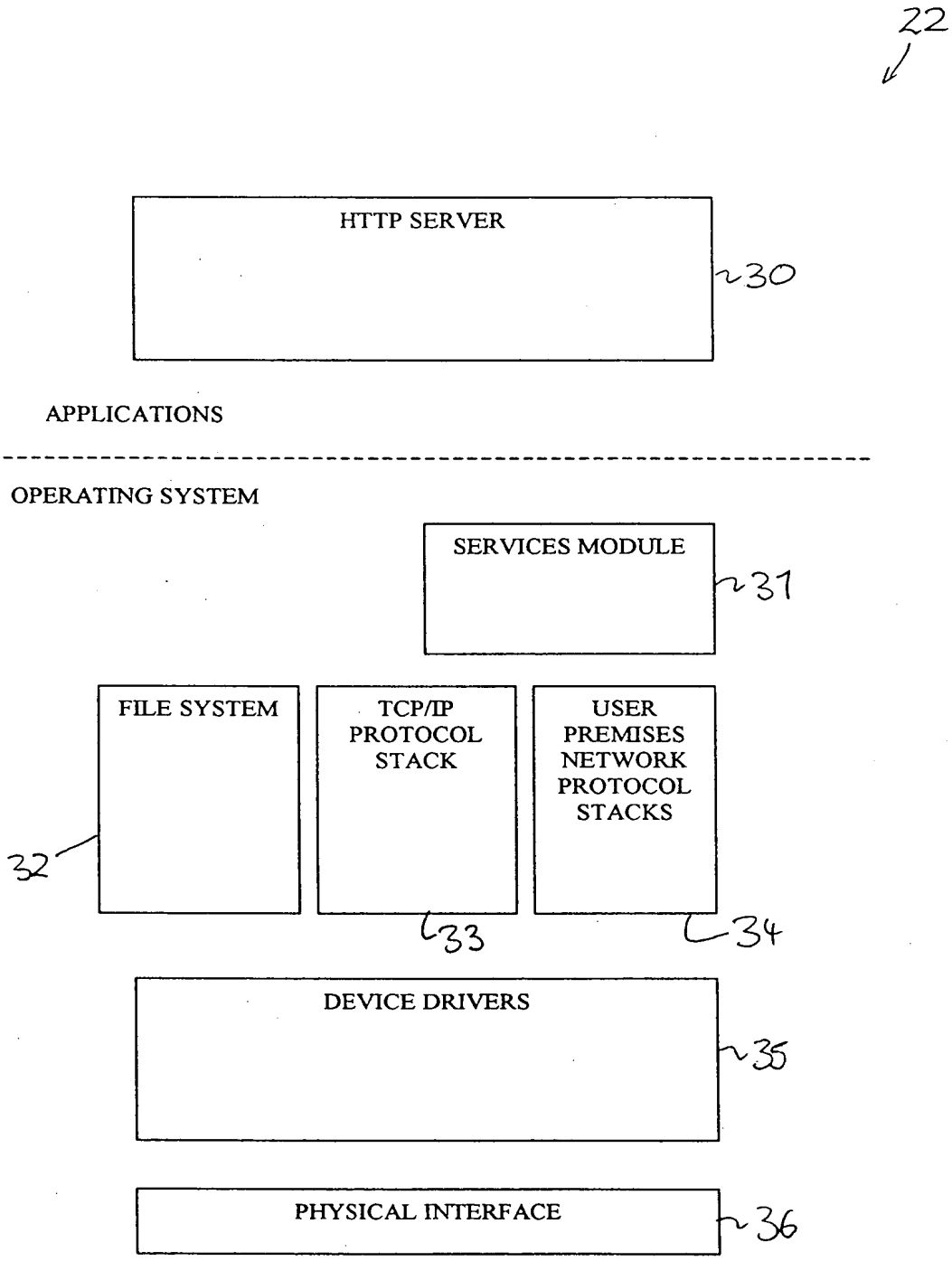
22
HTTP SERVER
30
APPLICATIONS
OPERATING SYSTEM
SERVICES MODULE
31
FILE SYSTEM
TCP/IP PROTOCOL STACK
USER PREMISES NETWORK PROTOCOL STACKS
32
33
34
DEVICE DRIVERS
35
PHYSICAL INTERFACE
36

FIG. 4

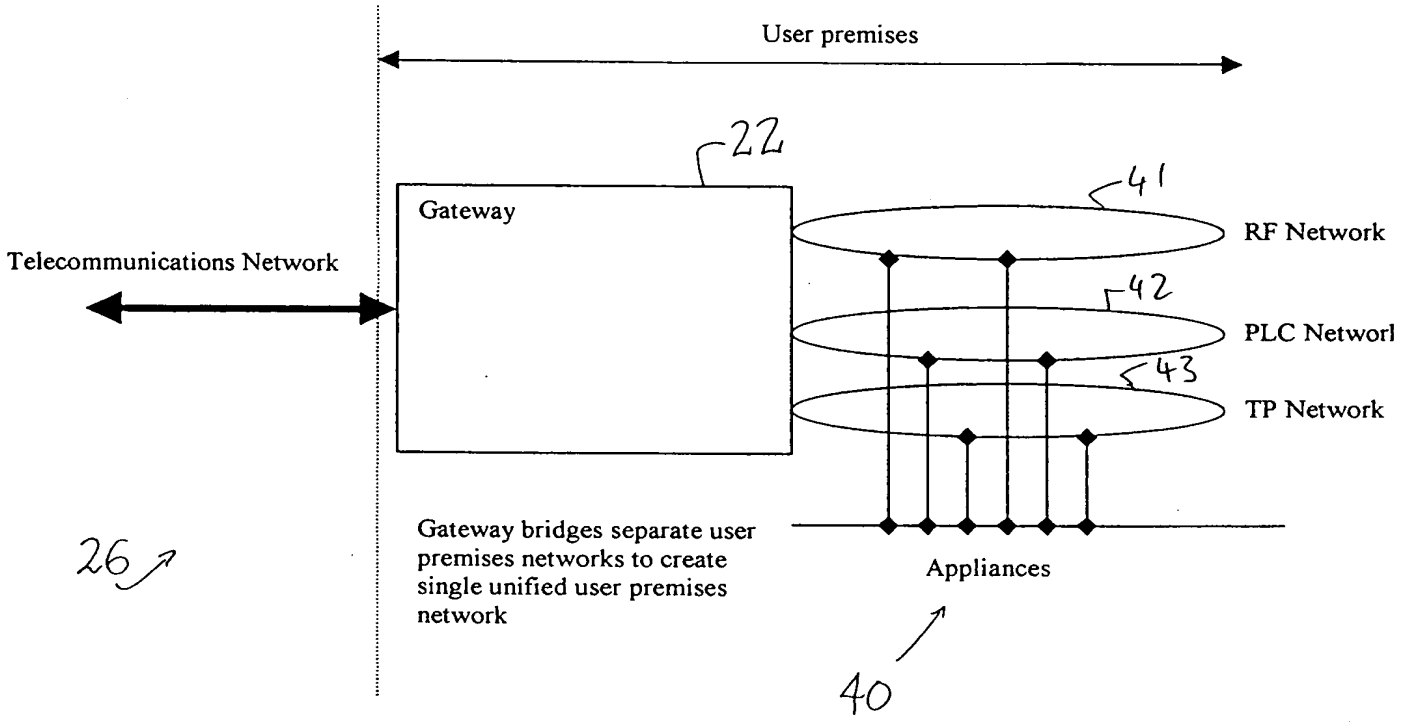
User premises
22
Gateway
41
RF Network
Telecommunications Network
42
PLC Networl
43
TP Network
26
Gateway bridges separate user premises networks to create single unified user premises network
Appliances
40

FIG. 5

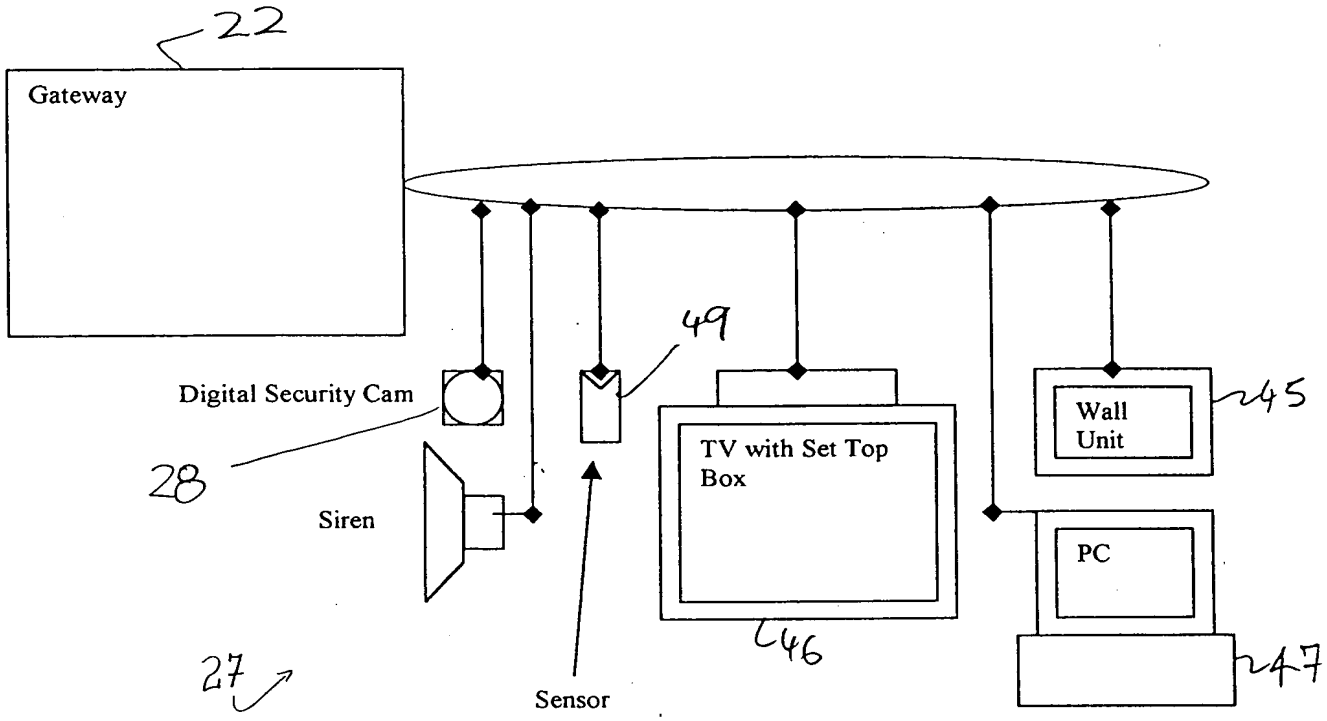
22
Gateway
49
Digital Security Cam
28
Siren
27
Sensor
TV with Set Top Box
46
Wall Unit
45
PC
47

FIG. 6

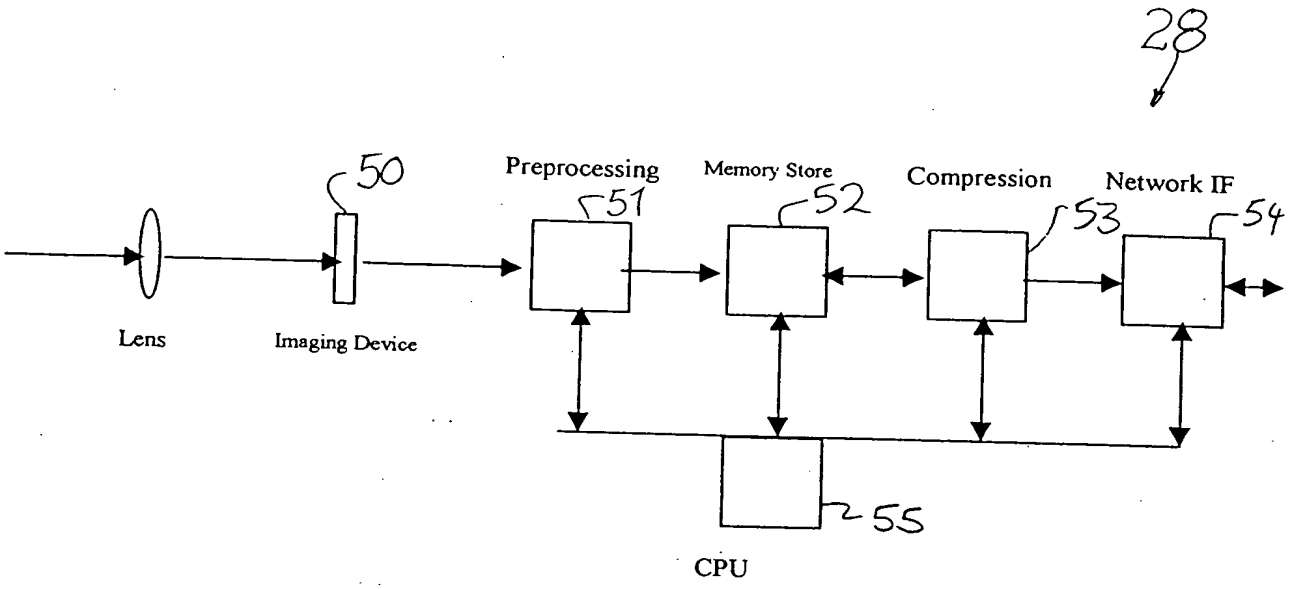
28
50
Preprocessing
Memory Store
Compression
Network IF
51
52
53
54
Lens
Imaging Device
55
CPU

FIG. 7

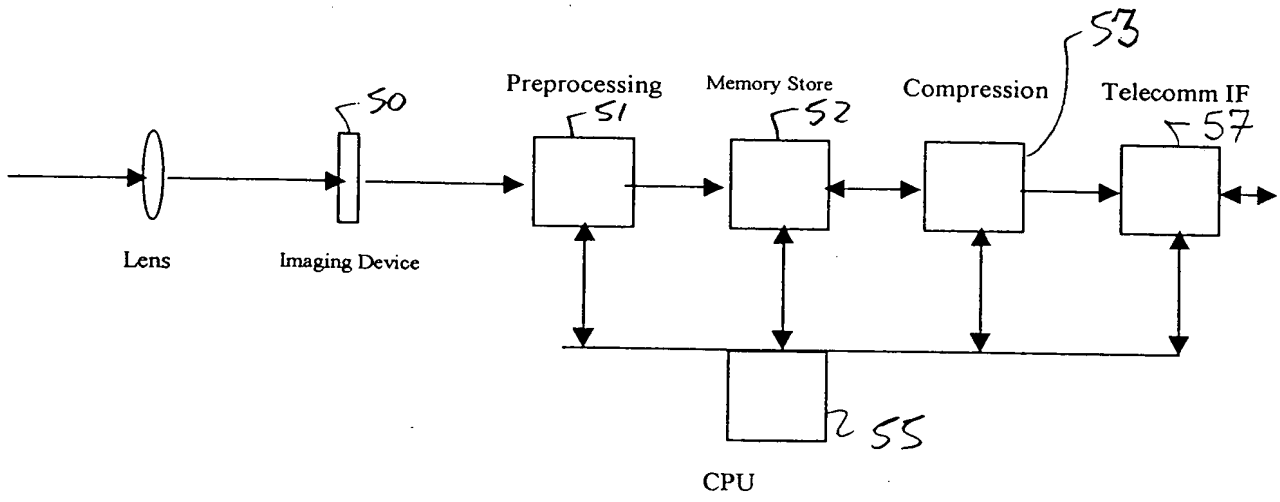
Lens
Imaging Device
50
Preprocessing
51
Memory Store
52
Compression
53
Telecomm IF
57
55
CPU

FIG. 8